Security of Quantum Key Distribution

Abdulbast Abushgra, Khaled Elleithy

Department of Computer Science & Engineering
University of Bridgeport, CT, USA

Abstract

Every day, the world looks on more of security analysis needs that are based on the enormous and sensitive information. This datum is shared by different systems around the world, which are considered at risk of attack at any time. Many scientists and researchers have brought up another cryptographic subject in Quantum Computing that is so-called Quantum Key Distribution (QKD) protocol. The first QKD is BB84 that was presented by Charles Bennett and Gilles Brassard in 1984. After that, several protocols were created sequentially with the same or different mechanism and with some abilities of these protocols to stand against well-known quantum attacks. This paper studies these protocols deeply and compares them to find the strong and weak points in each considered protocols.

Keywords

Quantum Key Distribution, Superposition, Entangled states, Pauli matrices, and Uncertainty.

Introduction

Cryptography has existed for several centuries as complicated algorithms, which are based on either exchanging or complicated mathematics functions. Now, the classical cryptography is the most used in a security system that depends upon public and private keys, which are initiated into difficult algorithms such as RSA, El-Gamal, or SHA. All these scenarios have been proved secure, but no longer if the scientists reached to establish quantum computer that will break all the previous algorithms just in seconds. Here, many of the computer scientists and physicians have been working on how to create a secret key in a quantum system the so-called Quantum Key Distribution (QKD). The first QKD protocol was announced in 1984 by Bennett and Brassard where this protocol is still the background point to come up with a new quantum protocol scheme. After that, several QKD protocols have been approved, some of which are protocol schemes that are very interesting and hold sparkling ideas in this field such as B92, SARG04, COW, KMB09 and EPR.

In this paper, we will discuss the most common quantum key distribution protocols and focus on the mechanism that is used in each protocol to extract the power and the weaknesses of each protocol.

Classical Cryptography

One of the challenges that faces the conventional cryptography is the security system that depends on the security of the shared key. Also, the speed of computer developments and its algorithms have become a threat to the shared and kept data, which should be secure[11]. The most famous mechanisms in the conventional cryptography are symmetric and asymmetric

cryptography that in general deal with several algorithms as a bit (0 or 1) or (true or false). Authentication is one of the requirements that should be fulfilled, and the used scheme starts mostly from the sender side who has the plaintext needed to be sent to the receiver[1]. Simply, we look at RSA as announced by Ron Rivest, Adi Shamir and Leonard Adleman in 1977, which is based on factorizing a large number from two prime numbers [18].

Moreover, El-Gamal's algorithm is considered an asymmetric key encryption algorithm as mentioned in his book [8] where the security in this algorithm depends on the difficulty of computing discrete algorithms.

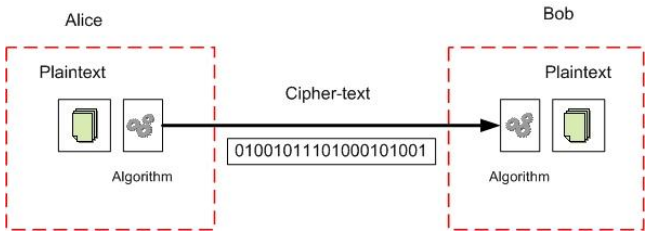

Figure (1). The conventional cryptography scheme.

Public key cryptography and RSA cryptosystem are called to the conventional cryptography, which in basically depends on the mathematical basis of the RSA. As mentioned above, RSA solves the communication between Alice and Bob by enciphering a key(public) and then deciphering the key (private) into complicated and flipped process [26]. This protocol has been approved as a secure protocol because Eve has problems computing a huge prime number that has been linked between Alice and Bob.

Quantum Cryptography

Quantum cryptography is guaranteed by the law of physics that demonstrates by non-cloning theory that supports unconditionally the secure key, and detects an eavesdropper over communicating quantum channel[22]. Generally, cryptosystems have been defined in three fields: designing cryptographic algorithms, which functionally leads the data to the desired target, developing encryption and decryption keys to control the algorithms, and distributes the secret key that connects parts of the communications[20]. This section of the paper will discuss the quantum key distribution protocols that have shown innovative ideas in how to create a secure mechanism between two parties.

1. BB84 Protocol

In 1984, Charles Bennett and Gilles Brassard introduced the new QKD protocol that is the so-called BB84 protocol. The BB84 protocol was designed to work on polarization states, which Alice (the sender) transmits randomlly independent photons to Bob (the receiver). Each basis in BB84 protocol reflects two values 0 or 1 that should be initiated in superposition[2]. Also, each state is shown in one of the two directions either rectilinear basis or diagonal basis. The rectilinear basis is polarized at 0^o or 90^o, while the diagonal basis is represented at 45^o or 135^o as shown in figure [1].

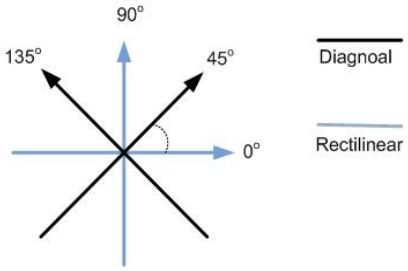

Figure (1) shows the polarization states in BB84.

BB84 protocol is often established in weakening coherent states in preparation states, which give a reasonable chance to be attacked by Photon-Number-Splitting attack(PNS)[28]. On the other hand, BB48's participants communicate with each other to get a secret key, when they wish to obtain the key in absence of Eve. Sending each bit in one of conjugate bases that Eve cannot know gives a protection. This protection comes based on the impossibility of measuring the state of a quantum system in two conjugate bases simultaneously[24].

The protocol as explained in [4] by Bennett and Brassard is the fundamental in quantum cryptography that the protocol highlighted the major ideas to how distributing a secret key. At first, Alice establishes creating random bits and then passes the desired bits into a quantum device to convert the bits to qubits. The qubit as mentioned by Noson S. Yanofsky and Mirco A. Mannucci in [27] is represented as a matrix, one column and two rows. This matrix would be 0 or 1, and it is called a state vector (space vector) as shown in function (1).

$$0 \rightarrow |0> \rightarrow \begin{bmatrix}1\\0\end{bmatrix}, \quad \text{or} \quad 1 \rightarrow |1> \rightarrow \begin{bmatrix}0\\1\end{bmatrix}. \tag{1}$$

Moreover, BB84 protocol is considered a simple and efficient protocol, where it can be used by some devices that are easy to find today. First, Alice chooses a random string of bits, which are encoded by a polarization device (Qubit). Then these qubits will be submitted into a quantum channel (fiber optics or free space) to Bob sequentially. After that, Bob randomly chooses the bases that he wants to measure the upcoming qubits by. Here in this paper, we will not discuss all the details about reconciliation or error correction; we just focus on the systematics of each protocol in this paper.

Alice bits	0	1	1	0	0	0	1	0
Alice Bases	+	×	+	x	+	x	+	+
Alice states	→	↖	↑	↗	→	↗	↑	→
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
Bob Bases	+	×	×	+	×	+	×	+
Bob State	→	↖	↗	→	↖	↑	↗	→
Bob Bits	0	1	0	0	1	1	0	0

Table (1). Sending qubits from Alice to Bob in BB84.

Several researchers came up with modifications to improve the BB84. For instance, Lo introduced in [14] the BB84 that was built in six states instead of four in the original scheme. Also, P. Shor announced an algorithm in [23] to improve the quantum reconciliation, of where to factor an odd number *n*, given a method for computing the order of an element. A random number *z* was chosen to find the order r_z of *z*, and then calculates GCD($z^{r/2}$ - *1*,*n*). Shor's algorithm is considered one of the most interested algorithms in quantum key distribution.

2. B92 Protocol

C.H. Bennett in 1992 [3] announced another QKD protocol that is based upon non-orthogonal states. The B92 is similar to the BB84 protocol, and the only difference is that it uses two states instead of four states. B92 protocol also was invented based on the Heisenberg's Uncertainty Principle that makes B92 unconditionally secure. Furthermore, B92 is a quantum key distribution protocol that uses two channels to extract the needed secret key. The first channel is a quantum channel that is employed to pass a polarized photons sequentially from Alice to Bob. The second channel is a classical channel that usually is used in QKD protocols to sift the qubits and then correct the occurred error [7].

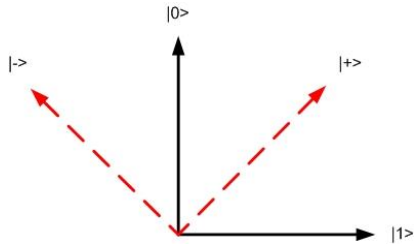

Figure (2). The states of photon in B92.

Here, Alice generates random bits, and she passes each single photon through one of the polarization direction. The first direction is a vertical (0) and the second is +45° (1). Bob on the other side has analyzers that are oriented in the horizontal direction (1) and -45° (0). Every time Bob measures a photon, there is a probability p = 50% of passing the photon through the analyzer. After Bob's measurements, he sends a copy of the measured photons to Alice. Either the photons were successfully passed or failed [17].

Alice bits	0	0	1	0	1	0	1	0
Alice qubits	→	→	↗	→	↗	→	↗	→
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
Bob Bases	x	+	×	x	+	x	+	+
Bob Observations	↖	→	↗	↖	↑	↖	→	→
Bob Bits	0	?	?	0	1	0	?	?

Table (2). Sending qubits from Alice to Bob in B92.

Note that Alice records the bit value (0) or (1) if she submitted |+> or |->, and Bob observes the value (0) or (1) if he got |-> or |+> [5].

3. SARG04 protocol.

SARG04 was introduced by Valerio Scarani et al. in [21] 2004. The SARG04 is known as robust QKD protocol against Photon Number Splitting (PNS) attacks. SARG04 and BB84 are equivalent in the quantum phase, while the variation is in encoding and decoding of the classical information [15]. The SARG04 protocol is described in several steps, which starts when Alice sends one of the two states in the set to Bob. Next, Bob measures the qubits by choosing one of the two bases randomly. After that Alice tells Bob which the state was chosen. Then Alice chooses some bits to test them, and Bob estimates the error rate e based on incorrect and correct received bits [9]. As a conclusion, Eve is not able to obtain information from single photon pulses[16].

4. Coherent One Way Protocol.

Coherent One Way Protocol was a solution for weak coherent pulses. As named COW, the protocol was presented by Nicolas Gisin et al.[10] in 2008. The COW protocol is summarized as follows. First, Alice starts sending a large number of time slots that include bit (0) and bit (1) with probability equal to *(1-f)/2*, and the decoy bits will be with probability *f*.

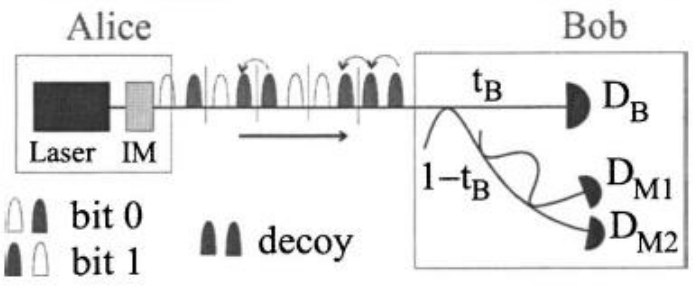

Figure (3). Coherent One Way Scheme.

After finishing the exchange of bits, Bob uncovers the bits that were obtained by the detector D_{2M} as shown in figure [3]. Next, Alice and Bob agree to remove bits that represent the decoy states (bits). Later, Alice estimates the break of coherent by computing the time slots to analyze the presence of Eve. At the end, Alice and Bob perform an error correction to end the communication with a secret key [25].

5. EPR Protocol.

In quantum mechanics, the EPR paradox is considered the most challenging ideas, which were started by Einstein, Podolsky and Rosen in 1935 [6]. The EPR protocol argued that quantum mechanics is not a complete physical theory. Moreover, the EPR pair is a two-qubit-system which is in one of the four Bell states. Bell states are entangled states of two-qubit-system [12].

$$|00\rangle_{ij} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j + |1\rangle_i |1\rangle_j)$$
$$|01\rangle_{ij} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |0\rangle_j - |1\rangle_i |1\rangle_j)$$
$$|10\rangle_{ij} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |1\rangle_j + |1\rangle_i |0\rangle_j)$$
$$|11\rangle_{ij} = \frac{1}{\sqrt{2}}(|0\rangle_i \otimes |1\rangle_j - |1\rangle_i |0\rangle_j)$$

Where |1> and |0> are eigenvectors of Pauli operators. Also, Alice and Bob agree that all the states above are encoded as [00, 01, 10 or 11] respectively. There are two legitimate parties, who initially share two EPR pair. The protocol is shown as if Alice holds particles (1, 4) and Bob holds (2, 3) from $|00\rangle_{1,2}$ and $|00\rangle_{3,4}$. Therefore, particles (1, 4) and (2, 3) are not in entangled states [13].

The EPR protocol starts with assigning both Alice and Bob one pair of entangled qubits. Then Alice and Bob separately pick a random sequence of bases to measure the particles. After that, they measure their qubits in desired basis. Publicly, both Alice and Bob compare the used bases, so that they keep just the bits that were measured in same basis.

Measuring the security and the efficiency of QKD protocols

The measurements that have been done in this paper are on two sides. The first measurement was applied to figure out the Run-Time for each QKD protocol. These protocols were evaluated by MATLAB and used QUBIT4MATLAB library. Furthermore, there are critical variations between each protocol such as handling the received qubits, measuring qubits in different bases, and correcting errors.

The second measurement is about the security of each studied protocol. The security function *j(k)* has been used to measure each protocol and its security level, where *j(k)* is equal to the natural logarithm with base *e* ~ 2.71828 of uncovered qubits divided by the length of qubit string[19].

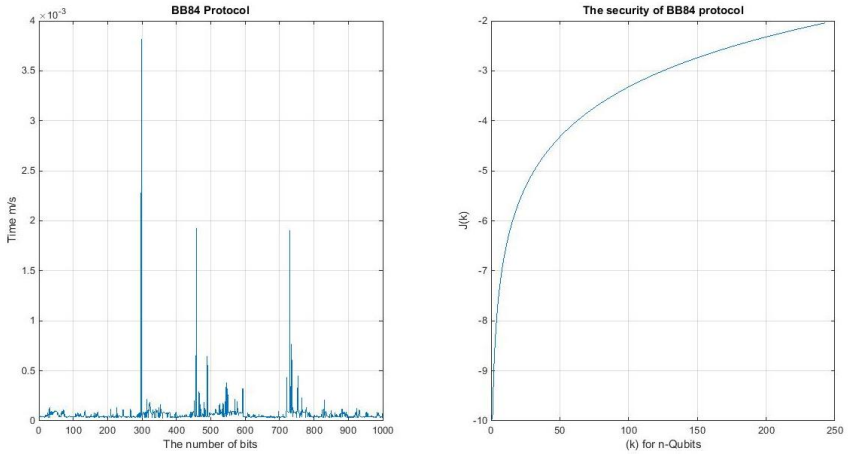

Figure (4). Shows the run time and the security of BB84 protocol.

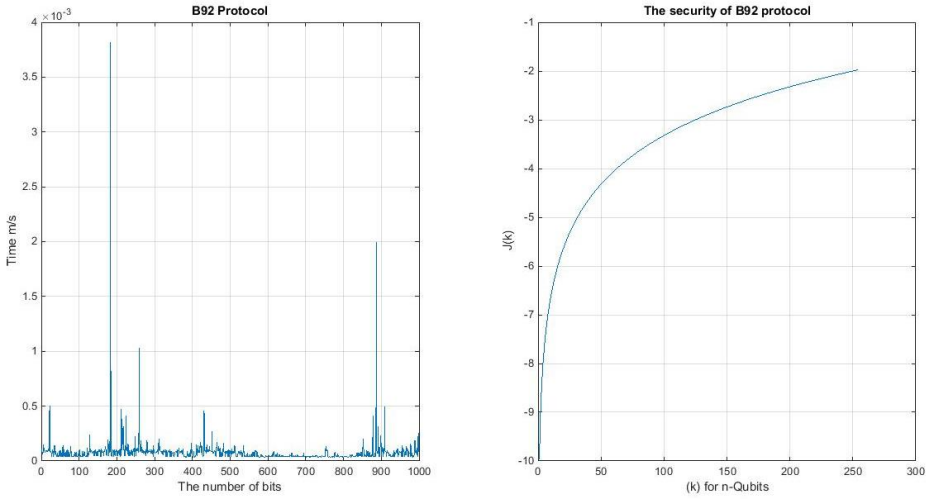

Figure (5). Shows the run time and the security of B92 protocol.

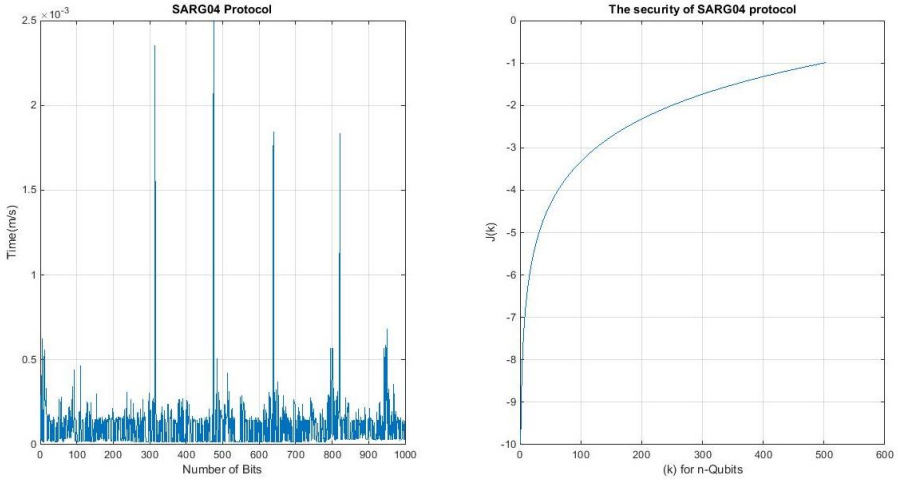

Figure (6). Shows the run time and the security of SARG04 protocol.

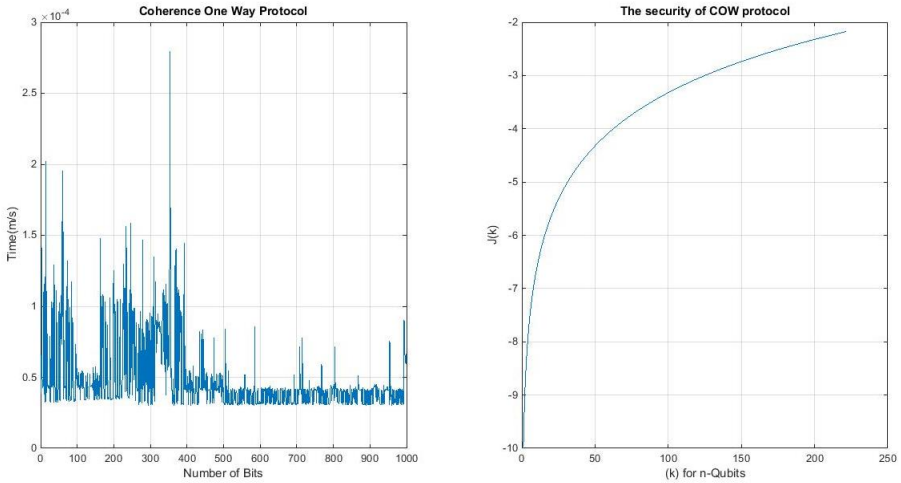

Figure (7). Shows the run time and the security of COW protocol.

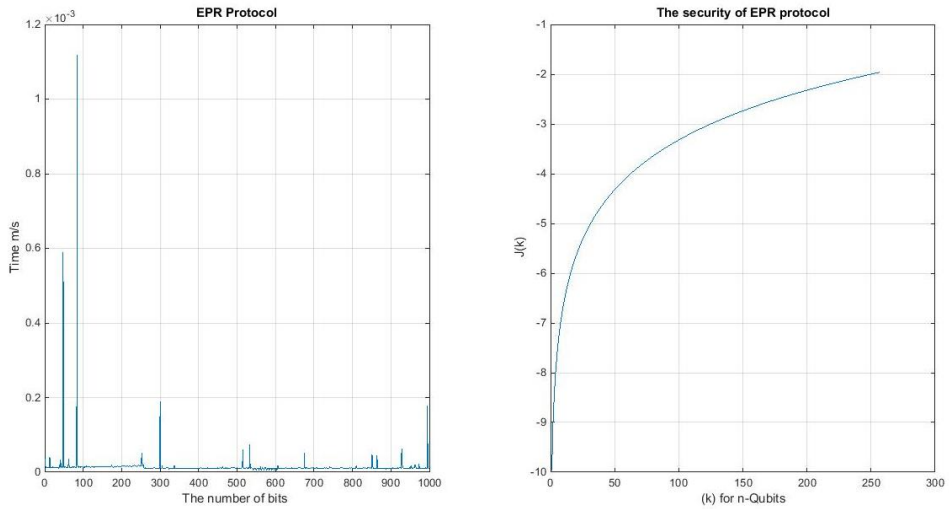

Figure (8). Shows the run time and the security of EPR protocol.

Conclusion

In this paper, several well-known QKD protocols were discussed to demonstrate the weak spots in QKD protocols and how they should be handled. Diagnosing these problems helps to modify or create QKD protocols that should be more efficient and have ability to stand against QKD attacks or the run time of algorithm complexity. The variations that are shown in the previous figures prove that there is a clear gap between each one of these protocols; especially in Run-Time execution. Each QKD protocol has different run time, which depends on the mechanism of handling the qubits. On the other hand, measuring the security of the studied QKD protocols demonstrates the rapprochement between these protocols. Finally, the QKD protocols are related to the laws of physics in quantum channel, but they are usually different in the classical channel.

References

1 H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, 'Authentication of Quantum Messages', in *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, 2002), pp. 449-58.

2 N. Benletaief, H. Rezig, and A. Bouallegue, 'Reconciliation for Practical Quantum Key Distribution with Bb84 Protocol', in *Mediterranean Microwave Symposium (MMS), 2011 11th*, 2011), pp. 219-22.

3 Charles H Bennett, 'Quantum Cryptography Using Any Two Nonorthogonal States', *Physical Review Letters*, 68 (1992), 3121.

4 Charles H Bennett, and Gilles Brassard, 'Withdrawn: Quantum Cryptography: Public Key Distribution and Coin Tossing', *Theoretical Computer Science* (2011).

5 Matthias Christandl, Renato Renner, and Artur Ekert, 'A Generic Security Proof for Quantum Key Distribution', *arXiv preprint quant-ph/0402131* (2004).

6 Albert Einstein, Boris Podolsky, and Nathan Rosen, 'Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?', *Physical review*, 47 (1935), 777.

7 Mohamed Elboukhari, Mostafa Azizi, and Abdelmalek Azizi, 'Quantum Key Distribution Protocols: A Survey', *International Journal of Universal Computer Sciences*, 1 (2010), 59-67.

8 Taher ElGamal, 'A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms', *Book* (1985), 10-18.

9 Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo, 'Performance of Two Quantum-Key-Distribution Protocols', *Physical Review A*, 73 (2006), 012337.

10 Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner, and Valerio Scarani, 'Towards Practical and Fast Quantum Cryptography', *arXiv preprint quant-ph/0411022* (2004).

11 Yin Heyu, and Xu Qiuliang, 'A Permanent Secure Qkd Protocol Realized with Asymmetric Key Authentication', in *Computational Intelligence and Security (CIS), 2012 Eighth International Conference on*, 2012), pp. 457-60.

12 Xiaoyu Li, and Liju Chen, 'Quantum Authentication Protocol Using Bell State', in *Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on*IEEE, 2007), pp. 128-32.

13 Zhihao Liu, Hanwu Chen, Wenjie Liu, and Juan Xu, 'Mutually Authenticated Quantum Direct Communication Based on Entanglement Swapping', in *Natural Computation (ICNC), 2010 Sixth International Conference on*IEEE, 2010), pp. 2984-88.

14 Hoi-Kwong Lo, 'Proof of Unconditional Security of Six-State Quantum Key Distribution Scheme', *arXiv preprint quant-ph/0102138* (2001).

15 L Moli-Sanchez, A Rodriguez-Alonso, and Gonzalo Seco-Granados, 'Performance Analysis of Quantum Cryptography Protocols in Optical Earth-Satellite and Intersatellite Links', *Selected Areas in Communications, IEEE Journal on*, 27 (2009), 1582-90.

16 L Moli, A Rodriguez, G Seco-Granados, and JA Lopez, 'Quantum Key Distribution (Qkd) Using Leo and Meo Satellites and Decoy States', in *Signal Processing for Space Communications, 2008. SPSC 2008. 10th International Workshop on*IEEE, 2008), pp. 1-6.

17 Fausto Montoya, 'La Criptografía Cuántica,¿ Realidad O Ficción?', *Instituto de Física Aplicada, Departamento del Tratamiento de la Información y Codificación, Consejo Superior de Investigaciones Científicas* (2004).

18 N. Muhammad, J. M. Zain, and M. Y. Mohd Saman, 'Loop-Based Rsa Key Generation Algorithm Using String Identity', in *Control, Automation and Systems (ICCAS), 2013 13th International Conference on*, 2013), pp. 255-58.

19 Marcin Niemiec, and Andrzej R Pach, 'The Measure of Security in Quantum Cryptography', in *Global Communications Conference (GLOBECOM), 2012 IEEE*IEEE, 2012), pp. 967-72.

20 J. Russell, 'Application of Quantum Key Distribution', in *Military Communications Conference, 2008. MILCOM 2008. IEEE*, 2008), pp. 1-6.

21 Valerio Scarani, Antonio Acin, Grégoire Ribordy, and Nicolas Gisin, 'Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations', *Physical Review Letters*, 92 (2004), 057901.

22 Zhao Sheng-Mei, Li Fei, and Zheng Bao-yu, 'A Proof of Security of Quantum Key Distribution in Probabilistic Clone Scheme', in *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003), pp. 1507-09 vol.2.

23 P. W. Shor, 'Algorithms for Quantum Computation: Discrete Logarithms and Factoring', in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, 1994), pp. 124-34.

24 Peter W Shor, and John Preskill, 'Simple Proof of Security of the Bb84 Quantum Key Distribution Protocol', *Physical Review Letters*, 85 (2000), 441.

25 Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden, 'Fast and Simple One-Way Quantum Key Distribution', *Applied Physics Letters*, 87 (2005), 194108.

26 IV Volovich, and Ya I Volovich, 'On Classical and Quantum Cryptography', *arXiv preprint quant-ph/0108133* (2001).

27 Noson S Yanofsky, Mirco A Mannucci, and Mirco A Mannucci, *Quantum Computing for Computer Scientists*. Vol. 20Cambridge University Press Cambridge, 2008).

28 Han Zheng-Fu, and Li Hong-Wei, 'Security of Practical Quantum Key Distribution System', in *Intelligent Signal Processing and Communications Systems (ISPACS), 2011 International Symposium on*, 2011), pp. 1-3.

Abdulbast Abushgra

He is a PhD student in Computer Science & Engineering at University of Bridgeport. He has served as professor assistant at Al-Mergib University in Libya since 2007. Also, he has worked in the Railroad Company for 10 years as an advisor. Now, his work focuses on the quantum security, and how to make a sharing secret key by Quantum Mechanics is possible in our classical system.

Khaled Elleithy

He is the Associate Vice President for Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundreds research papers in international journals and conferences in his areas of expertise.